Adapting Software-defined Information Centric Networks for IEC 61850-based Substations

Kuldeep Singh Shivran
Department of Electrical Engineering
Indian Institute of Science
Bengaluru, India
kuldeeps@iisc.ac.in

Sharad Shrestha
Computer Science Department
New Mexico State University
Las Cruces, U.S
sharad@nmsu.edu

George Torres
Computer Science Department
New Mexico State University
Las Cruces, U.S
gtorresz@nmsu.edu

Sarasij Das
Department of Electrical Engineering
Indian Institute of Science
Bengaluru, India
sarasij@iisc.ac.in

Satyajayant Misra
Computer Science and ECE Departments
New Mexico State University
Las Cruces, U.S
misra@nmsu.edu

2024 IEEE PES Innovative Smart Grid Technologies - Asia (ISGT Asia) | 979-8-3503-7392-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISGTAsia61245.2024.10876244

***Abstract*—A robust communication infrastructure is the backbone of power system efficiency and reliability advancements, enabling real-time data exchange and control. The smart grid, a complex network of digital devices, relies on their seamless communication to share information for monitoring, control, and protection. As the number of these devices and their communication needs increase, the role of software-defined and information-centric networking frameworks will become more pronounced for offering reliable and secure operation solutions. Given the time-sensitive nature and specific architecture of smart grid protocols, software-defined information centric networks (SD-ICN) can be appropriately designed to meet these requirements. SD-ICN can improve security by controlling access and authentication and efficient distribution of contents in the network. This paper explores recent SD-ICN structures and strategies to improve the reliability and security of communication in power systems substations. An IEC 61850-based substation networking architecture is presented to demonstrate the application of SD-ICN. Additionally, a mechanism to map the substation devices using Substation Configuration Language (SCL) to a routable Named Data Networking (NDN) name to route in the SD-ICN network is proposed.**

***Index Terms*—IEC 61850 Based Substation, Information Centric Networks, Named Data Networking, Smart Grid, Software Defined Networks.**

I. Introduction

The move from the traditional power grid to a smart grid is a significant advancement in energy production, distribution, and utilization. Efficient communication technology enables real-time monitoring, control, and optimization of the grid, while a secure and reliable communication mechanism is crucial for managing diverse grid components and ensuring the stability of modern power systems [1]. Conventional communication networks typically have a static configuration, where the control and data transfer aspects are closely integrated within network devices like switches and routers. This integration limits the network's ability to adapt to changing conditions and demand, making it challenging to manage and optimize traffic dynamically [2].

A network architecture with more flexibility and dynamicity can be found in Software-Defined Networking (SDN). In SDN, the control plane is decoupled from the data plane, allowing for centralized control and management of the network. The centralized controller can dynamically configure and optimize network resources, which leads to improved performance, scalability, quality of service (QoS), and security. Another architecture with the ability to meet the needs of the smart gird is Information-Centric Networking (ICN). ICN shifts communication from being location-based to content-based. In contrast to traditional IP-based communication, which routes traffic based on IP addresses, ICN routes traffic based on content names [3]. NDN is an architectural framework within the ICN paradigm that has been adopted for various smart grid applications because of its name-based content sharing, efficiency, and security features [4].

SDN and ICN offer significant advantages to the smart grid environment [5]–[7]. SDN offers dynamic, centralized control over network traffic, allowing for enhanced network management, improved security, and greater flexibility in handling network traffic. Meanwhile, ICN optimizes data retrieval, improves scalability, and reduces latency. These aspects enable SDN and ICN to address many limitations inherent in traditional network architectures.

In recent years, researchers have proposed a hybrid approach called SD-ICN, which combines the strengths of SDN and ICN. SD-ICN can enhance the resilience and scalability of smart grids [5], [6]. SD-ICN can protect from cyberattacks with dynamic security policies and real-time monitoring, enhancing data integrity. By utilizing name-based routing, which

This research was partially funded by the US National Science Foundation under grants #2148358 and #1914635, and the US Department of Energy grant #DE-SC0023392. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the US federal agencies.

is a feature of the NDN architecture, SD-ICN can address the challenges of smart grid interoperability caused by high rates of device proliferation and device heterogeneity. SD-ICN can optimize network resources, improve network performance, and reduce congestion through effective in-network caching. There are challenges in integrating these technologies with existing infrastructure.

SDN in substations enables centralized control, enhanced security, improved reliability, scalability, better QoS, and cost reduction. The centralized control model used by SDN can be a bottleneck for larger networks and a target for attacks. In ICN, managing and resolving content names can become overwhelmingly complex. This is especially true for systems such as smart grids, which consist of various levels and types of devices from different vendors, each with its own communication protocols. These factors also impose interoperability challenges on the existing substation system and communication infrastructure. This complexity underscores the need for efficient solutions, standardization, and strategies. Considering these challenges, the objectives of the paper can be defined as:

- Explore the benefits of SDN and ICN for IEC 61850-based smart grid substation applications.
- Propose an SD-ICN architecture for IEC 61850-based substations to ensure interoperability, reliability, security, and scalability, enabling the electricity grid to adapt to future technologies.
- Propose a standardized NDN naming convention using IEC 61850 Substation Configuration Language (SCL) files for scalable SD-ICN communication, incorporating message types to prioritize high-priority messages.

The rest of the paper is organized as follows. Section II presents an overview of the IEC 61850 standard, SDN, and ICN. Section III presents the benefits of SD-ICN in IEC 61850-based substation communication. In Section IV, we discuss the proposed SD-ICN architecture and its application in IEC 61850-based substations. Concluding remarks are summarized in Section V.

II. Overview

A. IEC 61850

Substations are crucial components of power systems that control and monitor power flow, and protect and maintain power system devices. Digital devices and communication capabilities enhance these functions for improved reliability and efficiency [8]. Protocols like MODBUS, DNP3, and IEC 60870-5-103 have served well in traditional substation communication but have limitations in terms of scalability, interoperability, and reliability. To address these issues, the Technical Committee (TC) 57 of the International Electrotechnical Commission (IEC) developed the IEC 61850 standard. This standard defines semantic data models, configuration languages, and communication protocols for substation automation [9]–[11]. Considering the needs of modern power systems, IEC 61850 is emerging as a more unified, flexible, and secure approach. It uses standardized data models and an object-oriented approach to enable seamless interoperability between multi-vendor devices. Additionally, IEC 61850 incorporates security features using IEC 62351 to enhance cybersecurity. IEC 62351 is a set of standards designed to secure communication protocols in power system automation, ensuring data integrity, confidentiality, and availability.

Interoperability, lower costs, improved reliability, and enhanced efficiency are the key features of the IEC 61850 standard. In this standard, logical devices group functions within a substation related to its physical host or another host in the network. As part of logical devices, logical nodes are defined with their datasets and associated functions. A Logical Node (LN) is a specific function or piece of functionality within a power system. Communication between nodes is facilitated through data exchange to perform specific tasks within the system. A client-server mode-based Manufacturing Message Specification (MMS) protocol is provided for communicating operational and configurational information to and from an IED. In IEC 61850-based networks, operational information messages, such as status and control, receive medium priority, while configurational messages, such as file transfer, have low priority. Generic Object-Oriented Substation Event (GOOSE) and Sampled Values (SVs) messages are defined as the highest priority messages. Binary data exchanges between IEDs for tripping, blocking, release, and indication are facilitated by GOOSE messages. Analog data, such as voltage and current samples, are sent to peer IEDs in the communication network using SV messages.

GOOSE and SV messages are considered critical messages and are directly mapped to the Ethernet layer for higher performance. The mapping of SV/GOOSE messages over the network and transport layer is defined in IEC 61850-90-5 to route them via WAN for centralized applications. R-SV/R-GOOSE messages refer to these messages when routed for centralized applications. The IEC 61850 standard now also extends to the system level, including renewables, wind, and generating stations. This standard provides an XML-based SCL. The SCL feature describes the substation and switchyard layout and the configuration of IEDs in terms of functionality, services, and communication addresses. The SCL files are System Specification Description (SSD), IED Capability Description (ICD), Substation Configuration Description (SCD), and Configured IED Description (CID) files, which specify the different levels of configuration and description of IEC 61850-based systems.

B. Software Defined Networking (SDN)

SDN is an architectural approach where a network is configured and controlled using software applications, making the network flexible. It emphasizes agile and flexible network management by separating network control logic from data forwarding [6]. The central controller provides a global view, making implementing and optimizing policies seamless. SDN employs open standards to ensure the interoperability and reliability of smart grids. For instance, SDN can improve the implementation of IEC 61850 by offering more flexible and efficient network management within substations. SDN can be used to utilize and construct secure, resilient, and high-performance Ethernet networks for IEC 61850-based Substation Automation Systems (SASs) and other Operational Technology (OT) applications [12].

SDN architecture is divided into three layers [13]. The top layer (application layer/plane) defines rules for various services, such as firewall, access control, IDS, QoS, routing, and monitoring. The middle layer (control plane) is an abstraction of network topology. The controller's tasks include setting up flow tables, defining data handling policies, simplifying network complexity, gathering network information, and keeping an updated network view. The bottom layer (data plane) encompasses networking devices such as physical or virtual switches, routers, and access points.

C. Information Centric Networks (ICN)

ICN is a novel network architecture that prioritizes the identification and retrieval of content by unique names. It enhances efficiency through fine-grained traffic control and built-in data security. NDN is a ICN architecture that retrieves and delivers content based on its name rather than its location. This shift from traditional IP-based communication enhances security, efficiency, and flexibility in data distribution [4]. NDN introduces components to improve network efficiency and security, including the Pending Interest Table (PIT) to track data requests, the Content Store (CS) to cache fetched data, and the Forwarding Information Base (FIB) to direct interests toward data sources. NDN is suited for smart grid applications which necessitate bidirectional communication flow [14] due to its efficient data distribution, enhanced security, and in-network caching that reduces latency and bandwidth usage for real-time operations [15]. The data-centric security model of NDN guarantees the authenticity and integrity of data, protecting communications within smart grids [16]. Its adaptable and scalable architecture enables the seamless incorporation of new devices and applications while supporting network resilience against disruptions.

Guo *et al.* [17] studied a name-based secure communication mechanism to enhance smart grid system security. The authors concluded that ICN/NDN can handle the security requirements of IEC 61850, including authentication, non-repudiation, integrity, access control, confidentiality, and authorization. GOOSE and SV in the IEC 61850 standard, which specifies a publisher/subscriber communication model, align well with the design of ICN/NDN. Operating at the physical and data link layers, GOOSE and SV are compatible with ICN/NDN by embedding NDN names within Ethernet frames, thereby enhancing efficiency and content retrieval. This compatibility instills confidence in the feasibility of the proposed solution.

III. Benefits of SD-ICN

SDN offers significant advantages for smart grid applications by enabling dynamic programming and customization of network components to meet the unique demands of smart grid environments. The centralized controller provides a comprehensive global network view, facilitating effective forwarding and routing decisions for optimized network performance, reduced latency, and reliability. In large-scale networks, SDN's centralized control can be distributed across multiple controllers to ensure scalability for modern smart grids.

SDN-based Smart Grid Communications (SGC) enable advanced functionalities such as substation automation and monitoring, automatic substation configuration, and the ability to meet Quality of Service (QoS) requirements. In their work, Rehmani *et al.* [18] listed several motivations for adopting SDN in smart grids: the isolation of different traffic types and applications, traffic prioritization, the creation of virtual network slices based on geographical or other domains, resiliency, fast failure recovery, interoperability among various communication networks, and enhanced fault detection. These capabilities make SDN an ideal framework for supporting modern smart grid infrastructures' complex and dynamic needs.

ICN/NDN also brings several benefits to the smart grid that can be attributed to NDN's strategy layer. The strategy layer exists between the Ethernet and application layers, enabling packet prioritization and precise routing decisions to be easily defined based on the content. This layer replaces the network and transport layers for MMS and serves as an additional layer for GOOSE and SV messages. QoS requirements can be met by taking advantage of the strategy layer as shown in [19]. This work uses a token bucket system and a weighted-fair queuing algorithm to ensure QoS for all priority levels. It also provides a DDoS mitigation system that effectively minimizes the attack's impact.

Zhang *et al.* in [6] highlighted the synergistic benefits of SD-ICN by illustrating how the strengths of one address the challenges of another. The challenges faced by SDN include unauthorized access, data modification, malicious applications, fake controllers, and DDoS attacks on switches and controllers. These issues can be effectively addressed by leveraging the benefits of ICN, which include self-certifying control messages, immutable data, and the prevention of host-based and data-based DDoS attacks. Other security risks in SDN are the vulnerability of its software for the control plane, the controller is a single point of failure, and the possibility of hijacking attacks where adversary can hijack the routes to the controller and replace them with routes to itself [20]. With ICN's data routing architecture and built-in data authenticity, the possibility of hijacking attacks is significantly reduced, while having a backup controller to replace a faulty one is a trivial exercise in ICN.

SDN's capabilities can address security challenges with ICN, such as expired content revocation and privacy. These include rapid revocation of expired content, maintaining an expired content list, centralized access control, and fast convergence to a consistent security configuration. The authors in [20] discuss how SDN can be used in a smart grid environment to detect malicious activities by analyzing packet traffic and how security can be improved by utilizing a virtual network to isolate suspicious switches. When used with ICN, attacks can be effectively mitigated by setting packet priority levels and rate-limiting certain entities in the system.

SD-ICN can significantly enhance the performance of IEC 61850-based smart grids by addressing key areas such as reliability, speed, security, scalability, and prioritization. These capabilities collectively make SD-ICN a robust framework for enhancing the efficiency, security, and scalability of IEC 61850-based smart grids. Despite these benefits, some technical challenges exist when deploying SD-ICN in the smart grid, such as the cost of deployment. Replacing existing IP architecture with ICN architecture may be quite a costly endeavor, along with adding the functionality to support SDN. Another challenge is the vulnerabilities that open up with a centralized controller. Attacks can focus on the SDN controller to bring down or severely impact the network. Other possible security concerns are spoofing legitimate control messages to send false instructions to the network and black hole attacks via malicious routing advertisements.

IV. Proposed SD-ICN Framework

A. SD-ICN Architecture

Figure 1 illustrates the proposed SD-ICN architecture tailored for IEC 61850, emphasizing the integration of SDN and ICN within the IEC 61850 standard. The architecture comprises three main layers: the Application Layer, Control Plane, and Data Plane. The Application Layer includes components for Substation Automation, Smart Grid Applications, Protection, Control, and Monitoring. The Control Plane features the SDN Controller, ICN Controller, Cache Management, and Network Management, responsible for managing network devices and content dissemination. The Data Plane consists of Network Devices, Content Stores, and Forwarding Mechanisms, ensuring efficient data routing and storage.

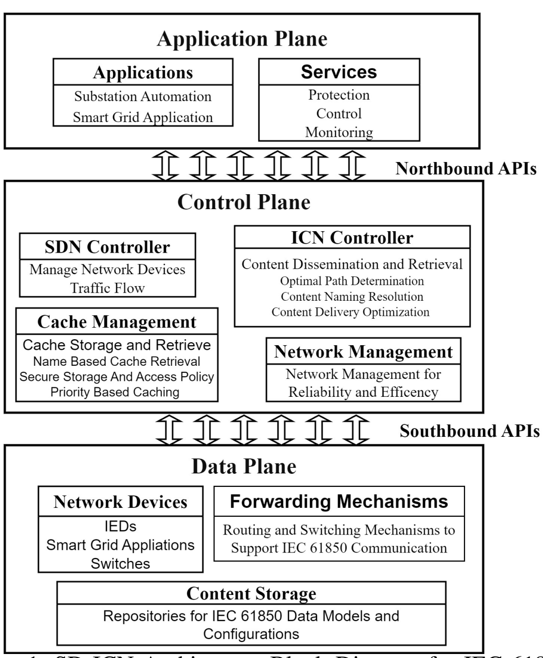

Fig. 1: SD-ICN Architecture Block Diagram for IEC 61850.

The southbound and northbound communication flows highlight how the control plane directs the data plane and relays feedback to the application plane. Communication between the application and control planes via northbound APIs demonstrates message transmission and feedback for IEC 61850 applications and services. Southbound APIs depict the interaction where the control plane manages the data plane with IEC 61850-specific commands and configurations. Furthermore, the data plane continuously provides status updates and feedback to the control plane, ensuring efficient operation and adherence to IEC 61850 standards.

SDN controllers can effectively manage ICN routers, allowing for dynamic configuration of routing strategies and cache policies to optimize network performance. In IEC 61850, a naming mechanism can be integrated into the ICN framework to manage and identify data objects in the power grid efficiently. This can be achieved using standardized IEC 61850 device names to label and retrieve content, ensuring seamless interoperability and enhanced security within the power grid.

B. SD-ICN Application

This section presents an IEC 61850-based communication topology that adapts SD-ICN-based communication for power system substations. We consider a simple single bus substation of 220/132 kV as a use case, referred to as T1-1 topology in IEC 61850 Part 5 [21]. Substation T1-1 consists of five bays: one transformer bay (D1Q1), a bus bay (E1Q4), and three line bays (E1Q1, E1Q2, and E1Q3), and two voltage levels (D1, E1). The substation communication network includes Human Machine Interface (HMI), SD-ICN controller, gateways, switches, and protection and control (P&C) Intelligent Electronic Devices (IEDs). P&C IEDs make decisions based on Merging Units (MUs) measurements and pre-defined protection and control settings for specific power system areas.

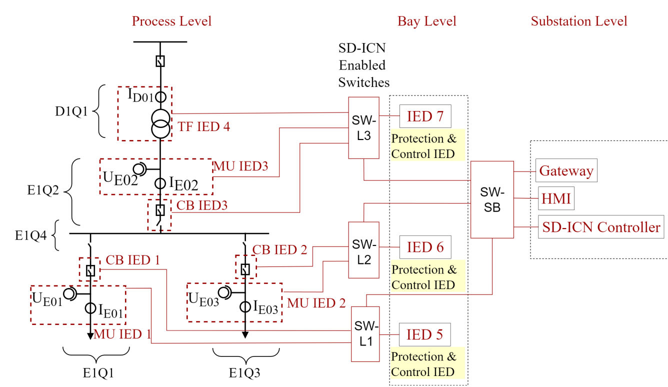

Fig. 2: T1-1 Substation with SD-ICN enable IEC 61850 based communication.

Figure 2 illustrates a simple IEC 61850-based communication topology for substation T1-1, which utilizes SD-ICN networking concepts. In this topology, bay one (D1Q1) is equipped with a transformer IED, bay two (E1Q2) contains a MU IED and a Circuit Breaker (CB) IED, bay four (E1Q1) contains two IEDs, and bay five (E1Q3) contains two IEDs. Additionally, Figure 2 showcases SD-ICN-enabled switches at the process bus, bay-level IEDs, an SD-ICN-enabled station switch, HMI, SD-ICN Controller, and Gateway. Process bus switches connect CB IEDs and MUs to communicate with Bay level IEDs, and station switches allow communication with substation HMI, control, and gateway.

As part of the SD-ICN architecture, naming conventions play a crucial role. This section outlines methods for addressing packets to endpoints, which may involve receiving messages, such as measurements, from or issuing commands to grid devices. A typical use case involves grid devices sending measurements to a P&C devices using SV messages and operational data using MMS to an aggregator or substation controller. A controller or operator sends control commands and configuration messages to grid devices. The operational and configuration-related messages can have more generic NDN names to take advantage of ICN content-based routing. An example of such aggregation is a substation control room aggregating information from IEDs for monitoring purposes using MMS message-based communication. For instance, the name 'MMS/Fault-Detection/Status/DeviceName/Controller' can be used for a grid device.

In the case of high-priority messages, such as SV and GOOSE, the names must be more specific for the traffic to be routed correctly to the device. For instance, "Message/Urgent-Control/IEDx/" could be used, where IEDx is the identity of a specific IED. The remainder of this section will explore the naming conventions for routing high-priority messages.

1) Standardization of NDN Name using IEC 61850 SCL Files: The SCD file in SCL is a file format used for data exchange from the system configuration tool to IED configuration tools. The SCD file contains information related to a single-line diagram, existing devices, including IEDs, access points, a communication configuration, and a substation description. SCL uniquely defines the names of substations and product parts, which form hierarchies [22], [23].

In ICN, data is retrieved by name and these names belong to one of the three categories: hierarchical, flat, and attribute-value pair-based. These names in ICN need to be unique, secure, user-friendly, and location-independent. NDN follows the hierarchical naming convention, where each name comprises multiple components arranged in a hierarchy. Hierarchical names in NDN uses longest prefix match for path resolution to the destination host.

The SD-ICN controller, as presented in Figure 2, can utilize NDN naming for each host in the network. The SD-ICN controller can use the information translated from SCD files to determine the position of existing devices in the substation communication network and their data flow for low-, medium-, and high-priority messages. The hierarchical order of the substation devices (from substation to process level) enables the SD-ICN controller to dynamically determine the naming convention for an IED. Thus, the hierarchy of names and mapping with functional and product structures in the SCD file helps create an interoperable, standardized, and scalable way to assign NDN names to devices and related messages.

2) A Naming Use Case for Substation T1-1: A portion of the SCD file for the T1-1 substation topology is illustrated in Figure 3. This shows the sections of the SCD file used to construct NDN naming for IEDs/MUs within the SD-ICN-based T1-1 substation communication network. A substation can have multiple voltage levels and bays. The annotations labeled with circled numbers in Figure 3 indicate specific substation elements. Annotation ① represents the substation named $S12$. Annotation ② represents a voltage level, $E1$, within substation $S12$. Annotation ③ represents bay two, labeled as $Q2$.

Fig. 3: Segment of the SCD file illustrating NDN naming for Bay 2 in Substation T1-1.

The SCD file contains a $pathName$, ④, associated with each $connectivityNode$ in a bay. This $pathName$ of the $connectivityNode$ specifies the location of each IED within the substation network, providing an absolute reference to the $connectivityNode$ to which each IED terminal connects. This allows the system configuration tool to map IEDs to their

TABLE I: NDN Names for SD-ICN based IEC 61850 GOOSE and SV Message Communication of Substation T1-1.

Substation	Voltage Level	Bay	IED Name	IED ID	NDN Name
S12	D1	Q1	TF IED4	D1Q1SB1	$GOOSE/S12/D1/Q1/D1Q1SB1$
			IED7	D1Q1BP2	$GOOSE/S12/D1/Q1/D1Q1BP2$
	E1	Q2	MU IED3	E1Q2SB1	$SV/S12/E1/Q2/E1Q2SB1$
			CB IED3	E1Q2SB2	$GOOSE/S12/E1/Q2/E1Q2SB2$
		Q3	MU IED2	E1Q3SB1	$SV/S12/E1/Q3/E1Q3SB1$
			CB IED2	E1Q3SB2	$GOOSE/S12/E1/Q3/E1Q3SB2$
			IED 6	E1Q3BP1	$GOOSE/S12/E1/Q3/E1Q3BP1$
		Q4	MU IED1	E1Q4SB1	$SV/S12/E1/Q4/E1Q4SB1$
			MU IED1	E1Q4SB2	$SV/S12/E1/Q4/E1Q4SB2$
			IED 5	E1Q2BP1	$GOOSE/S12/E1/Q2/E1Q4BP1$

locations in the substation topology, mirroring the hierarchy represented by annotations (1), (2), and (3). Additionally, the IED $name$, (5), a section of the SCD file, details the AccessPoint $name$ to which each IED is associated.

Let us consider an example IED named $CB\ IED3$, associated with a CB in bay two, to determine its NDN name from the SCD file. To operate this CB for protection, control, and maintenance, the operator or P&C, IED sends a control/trip-based GOOSE message to the associated IED $CB\ IED3$. Using the information from the SCD file explained in the previous paragraph and the naming convention of NDN, we can define the NDN name for $CB\ IED3$ as "GOOSE/S12/E1/Q2/E1Q2SB1" for GOOSE messages, which will be unique within the defined hierarchy. The GOOSE prefix in the NDN name helps switches assign high priority to the message in the NDN architecture. Then, to locate the $CB\ IED3$ in the network, the NDN follows the naming convention with the largest prefix match. Similarly, the NDN names for GOOSE and SV messages for other IEDs in the defined SD-ICN of substation T1-1 can be defined as mentioned in Table I. Also, an NDN name can be defined as "Substation/VoltageLevel/Bay/IED/LogicalDevice/LogicalNode" to communicate information between or from specific logical nodes. This name will be unique within that substation as determined from SCL files. So, using SCD files, SD-ICN can dynamically assign NDN names to IEDs, Logical Nodes within IEDs or other devices of IEC 61850-based substations in a scalable and standardized way, simplifying management, access, and scaling. In contrast, IP-based name resolution can face complex routing and dynamic IP management issues, impacting scalability and efficiency.

V. Conclusion

In this work, the IEC 61850 standard, SDN, and ICN for future-proof smart grids are discussed. These technologies can enhance the security, reliability, accuracy, and scalability of a power system's communication network. An overview of SD-ICN-enabled power grid substations is provided to demonstrate the application and benefits of SD-ICN in smart grids. A simple T1-1 substation with an SD-ICN-enabled IEC 61850-based architecture is presented, illustrating how SCD files assist the SD-ICN controller in defining the dynamic logical configuration of the substation. Additionally, it demonstrates how an SCD file can be used to uniquely determine the NDN name for ICN-based communication.

As future work, the security and scalability applications of SD-ICN-enabled substations will be explored. Additionally, the reliability of SD-ICN-based networks in smart grid can be studied.

References

[1] G. N. Ericsson, "Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, pp. 1501–1507, 2010.

[2] X. Dong, H. Lin, R. Tan, R. K. Iyer, and Z. Kalbarczyk, "Software-Defined Networking for Smart Grid Resilience: Opportunities and Challenges," in *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, CPSS '15, p. 61–68, 2015.

[3] R. Tourani, S. Misra, T. Mick, S. Brahma, M. Biswal, and D. Ameme, "ICENS: An information-centric smart grid network architecture," in *IEEE SmartGridComm*, pp. 417–422, 2016.

[4] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, K. Claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, "Named data networking," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 3, pp. 66–73, 2014.

[5] W. Rafique, A. S. Hafid, and S. Cherkaoui, "Complementing IoT services using software-defined information centric networks: a comprehensive survey," *IEEE Internet of Things Journal*, vol. 9, no. 23, pp. 23545–23569, 2022.

[6] Q.-Y. Zhang, X.-W. Wang, M. Huang, K.-Q. Li, and S. K. Das, "Software defined networking meets information centric networking: A survey," *IEEE Access*, vol. 6, pp. 39547–39563, 2018.

[7] Z. Ai, M. Zhang, W. Zhang, J. Kang, L. Tong, and Y. Duan, "Survey on the scheme evaluation, opportunities and challenges of software defined-information centric network," *IET Communications*, vol. 17, no. 20, pp. 2237–2274, 2023.

[8] J. C. Lozano, K. Koneru, N. Ortiz, and A. A. Cardenas, "Digital substations and IEC 61850: A primer," *IEEE Communications Magazine*, vol. 61, no. 6, pp. 28–34, 2023.

[9] R. E. Mackiewicz, "Overview of IEC 61850 and Benefits," in *IEEE PES General Meeting*, pp. 8–pp, IEEE, 2006.

[10] S. A. Gutiérrez, J. F. Botero, N. G. Gómez, L. A. Fletscher, and A. Leal, "Next-generation power substation communication networks: IEC 61850 meets programmable networks," *IEEE Power and Energy Magazine*, vol. 21, no. 5, pp. 58–67, 2023.

[11] M. Qureshi, A. Raza, D. Kumar, S.-S. Kim, U.-S. Song, M.-W. Park, H.-S. Jang, H.-S. Yang, and B.-S. Park, "A survey of communication network paradigms for substation automation," in *ISPLC*, pp. 310–315, IEEE, 2008.

[12] N. Kabbara, M. O. Nait Belaid, M. Gibescu, L. R. Camargo, J. Cantenot, T. Coste, V. Audebert, and H. Morais, "Towards software-defined protection, automation, and control in power systems: Concepts, state of the art, and future challenges," *Energies*, vol. 15, no. 24, p. 9362, 2022.

[13] K. Benzekki, A. El Fergougui, and A. Elbelrhiti Elalaoui, "Software-defined networking (SDN): a survey," *Security and communication networks*, vol. 9, no. 18, pp. 5803–5833, 2016.

[14] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," *IEEE communications surveys & tutorials*, vol. 14, no. 4, pp. 944–980, 2011.

[15] H. Dai, B. Liu, Y. Chen, and Y. Wang, "On pending interest table in named data networking," in *Proceedings of the eighth ACM/IEEE symposium on Architectures for networking and communications systems*, pp. 211–222, 2012.

[16] C. Yi, A. Afanasyev, I. Moiseenko, L. Wang, B. Zhang, and L. Zhang, "A case for stateful forwarding plane," *Computer Communications*, vol. 36, no. 7, pp. 779–791, 2013.

[17] L. Guo, M. Dong, K. Ota, J. Wu, and J. Li, "A name-based secure communication mechanism for smart grid employing wireless networks," in *IEEE Global Communications Conference*, pp. 1–6, 2016.

[18] M. H. Rehmani, A. Davy, B. Jennings, and C. Assi, "Software defined networks-based smart grid communication: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2637–2670, 2019.

[19] G. Torres, S. Shrestha, and S. Misra, "iCAD: Information-centric network architecture for DDoS protection in the smart grid," in *IEEE SmartGridComm*, pp. 154–159, IEEE, 2022.

[20] X. Dong, H. Lin, R. Tan, R. Iyer, and Z. Kalbarczyk, "Software-Defined Networking for Smart Grid Resilience: Opportunities and Challenges," *CPSS, ASIACCS*, pp. 61–68, 04 2015.

[21] P. CODE, "Communication networks and systems in substations–Part 5: Communication requirements for functions and device models," *ed*, 2003.

[22] International Electrotechnical Commission and others, "IEC 61850-6: Communication Networks and Systems for Power Utility Automation—Part 6: Configuration Description Language for Communication in Electrical Substations Related to IEDs," 2009.

[23] C. A. Vargas and C. Carmona-Rodriguez, "Software Defined Networking for electrical substations based on IEC 61850," in *IEEE Colombian Conference on Communications and Computing*, pp. 1–6, 2016.